UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática,* <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Pro Dialog, journal from the Polish CEPIS society PTI-PIPS

Cover page designed by Concha Arias Pérez
"Strategos" / © ATI 2008
Layout Design: François Louis Nicolet
Composition: Jorge Llácer-Gil de Ramales

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (April 2008)

"Model-Driven Software Development"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. IX, issue No. 1, February 2008

Monograph: IT Governance (published jointly with Novática*)

Guest Editors: *Dídac López-Viñas, Antonio Valle-Salas, Aleix Palau-Escursell, and Willem-Joep Spauwen*

UPENET (UPGRADE European NETwork)

CEPIS NEWS

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

COBIT as a Tool for IT Governance: between Auditing and IT Governance

Juan-Ignacio Rouyet-Ruiz

Cobit is establishing itself as an effective tool to set up IT Governance that will help IT departments convert themselves into technological partners of businesses. When analysing the suitability of Cobit for IT Governance we must be aware of its origins in auditing, and of its strengths and weaknesses resulting from such an origin. In this article we analyse Cobit's strengths and weaknesses as a framework for IT Governance, using as a reference another IT Governance model, that of Peterson.

Keywords: Alignment, Auditing, Cobit, IT Governance, Management of IT Services, Strategic Process Orientation.

Autor

Juan-Ignacio Rouyet-Ruiz has a degree in Telecommunications Engineering from the Technical University of Madrid (1997). He began his professional activity in the field of training consultancy in 1998. Since 2002 he has been involved in numerous ITIL implementation consultancy projects within key accounts, primarily in the Industrial and telecommunications sectors. In 2005 he joined Quint Wellington Redwood as an ITIL consultant, where he has been carrying out strategic consultancy activities in IT service management. As the person responsible for the quality of the training department in a multinational company he has successfully been through several AENOR audits. He has participated in IT service management congresses and conferences, and has published articles in that field. He is currently writing his doctoral thesis in the field of IT Governance. <i.rouyet@quintgroup.com>.

1 Introduction

In recent decades IT departments have been forced to evolve towards a necessary strategic alignment between the IT function and the business needs of the organization. Under this paradigm, IT departments have faced the situation of having to make a value proposition of their activity which is in line with the interests of the corporate management [1]. To that end the IT function is managed in three phases: it begins as a management model focused on the reduction of operational costs (technology provider); it then becomes a service organization, that seeks to satisfy the necessities of its clients (service provider); and it ends up as a business partner offering valuable solutions and seeking the interest of stakeholders as well as growth in market turnover or penetration (technology partner) [2].

In this article we focus on management in terms of the last IT function. From a theoretical perspective, such an alignment is achieved with Henderson and Venkatraman's SAM model [3]. The next step consists of being capable of carrying out this strategic alignment from a practical point of view, for which elements such as IT Governance are necessary.

Currently one of the main models for IT Governance is Cobit, a model rooted in auditing. This origin in auditing gives Cobit characteristic strengths and weaknesses. In this article we will analyse the suitability of Cobit for IT Governance. To do that, we will study in some detail what is understood by IT Governance, and we will compare Cobit with Peterson's IT Governance model.

2 The Concept of IT Governance

In order to clearly define and understand the concept of IT Governance, we must first be aware that it fits within the practices and regulations of corporate governance. According to the OECD (Organization of Economic Co-operation and Development) corporate governance aims to establish *responsibilities* to *assure* objectives and measure performance [4]. Such performance is related with the *creation of value* for the organization and the *management of its resources* in an efficient and transparent way. This leads us to the four elements that make up corporate governance: responsibility, guaranteeing objectives, creating value and resource management.

These same four elements must be applied to the IT function, especially taking into account the direct implications that technology and its management currently have on business processes. From under these basic assumptions, therefore, the concept of IT Governance emerges as a subset of corporate governance. There is currently no consensus about exactly how to define IT Governance, although it is true that the various definitions have common elements.

We can begin with the definition provided by MIT (Massachusetts Institute of Technology), through its *Sloan School of Management's Center for Information Systems Research* (CISR), which points out that *IT Governance specifies the decision making rights and the framework of responsibilities to promote desirable behaviour in the use of IT* [5]. Notice that this definition is clearly focused on decision making, but does not define what to decide, calling it simply *desirable behaviour* in the use of IT.

Another definition is taken from Wim Van Grembergen, according to whom IT Governance is *the capacity to organize, executed by the board of directors, executive management and IT managers, to control the formulation and implementation of the IT strategy and, in this way, ensure the fusion of business and IT function* [6]. As can be seen, this definition is focused on defining who is primarily responsible for IT Governance, and pays special attention to searching for alignment between the IT function and the business.

Finally we provide the definition offered by the *IT Governance Institute* (ITGI), the body that created Cobit: IT Governance *is the responsibility of the board of directors and executive management, and consists in leadership and organizational structures and processes that ensure that the IT function of the company sustains and extends the organization's objectives and strategies* [7]. As can be seen, this definition is also focused on who must assume the responsibility for IT Governance, at the same time that it indicates in greater detail the activities and structures that make it up. It also defines more precisely what Van Grembergem called the *fusion of business and the IT function*, which, according to ITGI, consists in the IT function sustaining and extending the organization's objectives.

These definitions make it apparent that there are various points of view of IT Governance, and it may therefore be that we do not have a clear idea of what it is exactly. To obtain an overall view we can refer to Table 1, in which IT Governance is compared to corporate governance.

Just as there are different definitions of IT Governance, there are just as many practical models for its implementation because the concept of IT Governance is difficult to classify in a simple collection of processes or mechanisms. The lack of a single model means we need, at least, a framework to indicate *what* should be considered, leaving *how* such considerations should be taken into account to the private interpretation of each model. To arrive at some consensus on the common objectives of IT Governance we can refer to Forrester, an independent IT consultancy of recognised prestige. According to that organization, the objectives of IT Governance are: IT function value and alignment, risk management, performance measurement, and responsibility [9], which are all aligned in some way with previously indicated objectives established by the OECD.

We will analyse Cobit based on these objectives and using the IT Governance model of Peterson as a reference.

3 Peterson's IT Governance Model

Peterson [10] establishes a framework that indicates what aspects must be taken into account to implement IT Governance, leaving to the choice of each company exactly *how* to implement it. In search of a performance framework, this author establishes that IT Governance must be implemented according to a set of structures, processes and relational mechanisms. Structures are understood as the existence of a set of responsibilities; processes refer to decision making and performance measuring activities; finally, relational mechanisms make clear the need for the IT function to participate in the business and favour communication (see Table 2).

Achieving Forrester's previously listed IT Governance objectives, Peterson's model focuses on the definition of responsibilities and on risk management, achieved mainly through the definition of the structures and the relational mechanisms. The measurement of performance would appertain more to the field of processes. However, it does not establish clear mechanisms to define the IT function's value and alignment with the business.

4 Cobit as a Model of IT Governance

Cobit was developed by the *Information Systems Audit and Control Association* (ISACA), through the *IT Governance Institute* (ITGI), as a management auditing mechanism for IT departments, and over time has become a standard for IT Governance. The Cobit acronym stands for *Control Objectives for Information and Related Technology*, which indicates the way Cobit should be considered: as a system that facilitates IT management controls.

According to ITGI [7], Cobit supports IT Governance by creating a framework that covers the following five areas: strategic alignment, value delivery, resource management, risk management and performance measurement. To that end, it establishes four courses of action: focused on the business, directed towards processes, based on controls

Responsibilities of Corporate Governance	Responsibilities of IT Governance
▪ How do shareholders get executives to return some profit?	▪ How does advanced management get the IT director and the IT to return value from the business?
▪ How do shareholders make sure executives do not waste the capital lent in loss-making investments or projects?	▪ How does advanced management make sure the IT director and the IT do not waste capital in loss-making investments or projects?
▪ How do shareholders control executives?	▪ How does advanced management control the IT director and the IT?

Table 1: Corporate Governance and IT Governance [8].

	Structures	Processes	Relational mechanisms	
Tactics	▪ IT board of directors ▪ Committees	▪ Making strategic IT decisions ▪ Monitoring the IT strategy	▪ Participation of all concerned (*stakeholders*) ▪ Business-IT association	▪ Strategic dialogue ▪ Shared learning
Mechanisms	▪ Roles and responsibilities ▪ Organizational structure of the IT ▪ IT director on the Management Council ▪ IT strategic committee ▪ IT management committees	▪ Strategic planning of Information Systems ▪ IT balanced scorecard (*IT BSC*) ▪ Economic information ▪ Service level agreements ▪ COBIT and the ITIL ▪ IT Governance maturity models	▪ Active participation of those primarily concerned ▪ Collaboration between those primarily concerned ▪ Compensation and incentives for business-IT association ▪ Joint business-IT siting	▪ Shared understanding of the business and the IT objectives ▪ Active conflict resolution (not avoided) ▪ Inter functional business-IT training ▪ Inter functional business-IT job rotation

Table 2: Structures, Processes and Mechanisms of Relation for the Implementation of IT Governance [10].

and guided by metrics.

The main idea of Cobit is to make available a series of processes that will help manage and control the IT function resources, and make sure the business receives the information it needs to achieve its objectives. To define how the information should be, Cobit establishes a series of requirements the information must meet to be satisfactory for the business, which it calls *information control criteria*: effectiveness, efficiency, confidentiality, integrity, availability, compliance (of laws, regulations, etc.) and reliability.

With regard to its process direction, Cobit offers a set of processes grouped into four blocks of activities: planning and organization (PO), acquisition and implementation (AI), delivery and support (DS) and monitoring and evaluation (ME).

Finally, in order to be based on controls and guided by metrics, Cobit defines the *IT control objectives* as a declaration of the desired result or of the objective to attain through the implementation of control procedures in a particular IT activity. The Cobit metrics feature three measurement elements: maturity models, performance metrics and activity objectives, of which, the performance metrics are the best known.

The performance metrics are established in two groups: the key goal indicators (KGI) and the key performance indicators (KPI). Along these lines, the diagram of performance metrics grouped on three graduated levels is well known: those that measure if the goals of the IT function have been fulfilled (IT KGI), those that measure the fulfilment of the IT process goals (process KGI), and finally those that measure the performance of such processes (process KPI). This chain of measurements makes Cobit more business oriented, since that the impact that a process has on the business can be monitored from the lowest to the highest level.

5 Conclusions

According to the OECD, corporate governance should focus on four elements: establishing responsibilities, attaining goals, creating value and managing resources. Adapting these goals to the IT environment, Forrester proposes the following five elements: IT function value, alignment, risk management, performance measurement and responsibility definition. In terms of these principles, Cobit shows great strength with regard to performance measurement, value creation and risk management.

To be sure, due to its metrics structure, grouped in IT KGI, process KGI and process KPI, the performance measurement of the IT activity is kept totally under control. To the degree that the IT function is able to demonstrate its performance, it also shows its value to the business, given that value demonstration is currently and unfailingly connected to quantitative terms. In the same way, the strong measurement control makes sure the risks of diversion from objectives are also controlled, which is why Cobit also features great strength in risk management.

These three strengths are sustained in two characteristic aspects of Cobit: its origins in consultancy and its orientation towards process. Its origins in consultancy are the result of having the so-called *control objectives* of the processes and *control criteria* of the information. The first guarantees the minimum requirements each process must meet; the second guarantees that the information is that which the business needs. Notice that both cases deal with control, as this is the foundation for measuring performance and managing risks. And we must not forget the very meaning of Cobit (*Control Objectives for Information and Related Technology*), which indicates how Cobit should be considered: as a system that facilitates information and technology controls. The orientation towards processes structures the entire set well.

The system of nesting metrics, which makes a KGI from one level become a KPI from a higher level, provides the necessary mechanism for a correct alignment of the IT function. Through the Cobit metrics it is possible to "see" the importance of a performance measurement (KPI) in the IT goals. That is, a relationship is seen between process activities and their influence over IT goals, which leads to alignment.

But it is here, in this point, where the weaknesses of Cobit also begin to appear. We talk about alignment, but we must point out that such an alignment remains within the IT. Indeed, as we have seen, Cobit shows great strength in establishing suitable controls so that the IT activities are attuned to IT goals. The weak point lies in the link between IT and business goals. As can be seen in Appendix I [7] of Cobit, once the goals of the business are known, the relation with the IT goals is achieved by selecting a series of processes. This can produce indetermination as well as of rigidity.

Rigidity comes from having to establish some processes according to the strategy, when it is known that stable processes should be established over time, and be sufficiently flexible in their goals and performance measurement to be adapted to any strategy. The indetermination originates in the fact that Cobit neglects aspects related to taking responsibilities and the relational mechanisms that guarantee the alignment with the corporate strategy. These structures of responsibility and relational mechanisms go beyond the RACI matrixes defined by Cobit and focused on the interior of the IT, but they do not establish mechanisms so that the IT is one more element in the Management Committee, a true governing element.

Thus, Cobit's origins in auditing makes it a perfect frame of reference for the internal control of IT, guaranteeing performance measurement, value creation and risk management. These fields are defined in Cobit's process orientation and in the structured metrics system that measures those processes. From our point of view, the aspects that must be improved revolve around the establishment of responsibilities and alignment with the business strategy. For those aspects we consider most difficult to grasp, we could refer to Peterson's IT Governance framework, which establishes elements for governance structures and relational mechanisms, the elements that finally control the formulation and implementation of the IT strategy based on the business strategy.

References

[1] N. Kriebel, P. Matzke. Building Meaningful Business Value Propositions. Forrester, August, 2006.

[2] O. Le Gendre. IT Departments and IT Governance. Gartner, IT Governance Forum-June, 2001.

[3] J.C. Henderson, N. Venkatraman. Strategic Aligment: Leveraging information technology for transforming organizations. IBM System Journal, Vol 38 - Nº 2&3, 1993.

[4] OCDE. Principles of Corporate Governance. OECD, París, 2004.

[5] P. Weill, J.W. Ross. IT Governance: How top performers manage IT decision rights for superior results. Harvard Business School Press, Boston, Massachusetts, 2004. ISBN: 1591392535.

[6] W. Van Grembergen. Structures, processes and relational mechanisms for Information Technology Governance: Theories and practices en Strategies for Information Technologies Governance. Hershey: Idea Group Publishing, 2003. ISBN: 1591401402.

[7] IT Governance Institute. Cobit 4.0. Rolling Meadows: IT Governance Institute, 2005.

[8] T. Sheleifer, W. Vishny. A survey on Corporate Governance. The Journal of Finance, 52(2), 1997.

[9] C. Symons. IT governance framework. Forrester, March, 2005.

[10] R. Peterson. Information strategies and tactics for Information Technology governance, en W. Van Grembergen (Ed.), Strategies for Information Technology Governance. Hershey, PA: Idea Group Publishing., 2003. ISBN: 1591401402.